UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/071,455	02/08/2002	Shaheed Bacchus	50325-0631	9956

29989 7590 08/10/2006

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 08/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/071,455	BACCHUS ET AL.	
	Examiner	Art Unit	
	Thomas M. Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 April 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 are pending.

2. The amendment of 4/27/06 have been received and entered.

Response to Arguments

3. The Applicant has argued on page 13:

A statement by an applicant during prosecution identifying the work of another as "prior art" is an admission that the work is available as prior art against the claims. Similarly, where the specification identifies work done by another as "prior art," the subject matter so identified is treated as admitted prior art. See MPEP 2129 (citing cases).

The Examiner has found Applicant's citation pertinent and relevant to the issue of identifying information as admitted prior art. Accordingly, the Examiner has withdrawn the rejection of the admitted prior art which was available under 35 USC 102.

The Applicant has argued on pages 17-18:

Specifically, Stallings does not teach, suggest or describe a) a mapping of encryption types to a list of one or more available onlines services, b) determining an encryption type match by matching the list of encryption types received from the client to a list of encryption types

contained in the mapping, c) selecting an online service based on the encryption type match and the list of one or more available online services associated with the encryption type match.

The mapping of online services to encryption types is established prior to any communication between the client and the server. For example, an administrator determines the mapping of online services to required levels of encryption. The mapping of services to encryption types determines what services, if any, a client can obtain in the approach of claim 1. Nothing in Stallings discusses a mapping of online services to encryption types.

With this basic view, the Examiner disagrees. Page 452 of Stallings recites that the CipherSuite contains a list that contains the combinations of cryptographic algorithms supported by the client, in decreasing order of preference. It is evident then that each of these algorithms corresponds with the actual service of being able to encrypt using that particular algorithm. If DES is chosen from the list(page 453), then the service of encryption using DES will be used. If RC4 is chosen instead, then RC4 will instead be used. For the purposes of examination, the Examiner has construed the encryption algorithm to be an online service because these encryption algorithms are being used to negotiate and secure an online transfer of data from a server to a client.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-3, 5-8, 10, 14-17, 19-26 are rejected under 35 U.S.C. 102(b) as being anticipated by "Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security".

In reference to claim 1:

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" discloses a method of providing data from a service to a client over a telecommunication network based on encryption capabilities of the client, the method comprising the computer-implemented steps of:

- Receiving from the client a request for data and a list of encryption types representing encryption capabilities that are available at the client, where the request from the client is the client hello, and the list of encryption types is the cipher suite which is the list containing the combinations of cryptographic algorithms supported by the client. (pages 451-452)
- Determining an encryption type match by matching the list of encryption types received from the client list of encryption types to a mapping of encryption types to a list of one or more available online services, where the ciphersuite contains a list of supported encryption algorithms list provided by the client and where the list contains the encryption algorithms that are available or "available online services" (pages 451-453) and the server determines an encryption type match by selecting one of the supported encryption types from the list to use. (page 452, 1st and 2nd paragraph)

- Selecting an online service that can provide the data to the client based on the encryption type match and the list of one or more available online services associated with the encryption type match, where the selection of the service is performed in the server_hello message and a ciphersuite is selected by the server from the list provided by the client. (pages 451-453) & (page 452, 1st and 2nd paragraph)
- Causing communication of the data from the selected online service to the client, where the server_hello message is communicated to the client. (Figure 14.6) & (pages 451-453)

In reference to claim 2:

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" discloses a method as recited in claim 1, further comprising the step of establishing a secure connection with the client, and wherein the receiving step is carried out as part of the establishing step, where the receiving step of receiving from the client a request for data establishes a number of parameters to how the secure connection is to be instigated. ("Phase 1. Establish Security Capabilities, page 451)

In reference to claim 3:

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" discloses a method as recited in claim 1, further comprising the step of establishing a secure connection with the client, and wherein the receiving step is carried out as part of the establishing step, wherein the secure connection is established using a security protocol selected

from among the set consisting of SSL, PPTP, SSH, and IPSec, where the security protocol that is selected is SSL.

In reference to claim 5:

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" discloses a method as recited in claim 1, further comprising the step of establishing a secure connection with the client, and wherein the receiving step is carried out as part of the establishing step, and further comprising the step of disconnecting the secure connection and reestablishing the secure connection using a cipher suite match, where the disconnection and the reestablishment of the connection is the Phase 2, Server Authentication and Key Exchange, and the disconnection is made by the server_done message which is always required. (pages 451-454) & (Figure 14.6) The re-establishment of the connection is made in Phase 3.

In reference to claim 6:

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" (pages 451-454) discloses a method as recited in claim 1, wherein the ordered mapping of encryption types to services is an ordered mapping of cipher suites to services, where the cipher suit is an ordered list of encryption types, and where these particular encryption types are cipher suites that are mapped to their respective encryption or hashing services(RSA, Fixed Diffie Hellman, etc.)

In reference to claim 7:

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" discloses a method as recited in claim 1, further comprising the steps of receiving a weight value for one or more of the encryption types and ordering the mapping of encryption types to services based on the received weight values, where the weight value is the preference as set by the client, and the encryption types are ordered based on this value. (pages 452)

In reference to claim 8:

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" (pages 451-454) discloses a method as recited in claim 1, wherein the encryption type is a cipher suite match.

In reference to claim 10:

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" discloses a method as recited in claim 1, wherein the step of causing communication further comprises the step of establishing a connection with a non-encrypted protocol for use in communicating a request to the selected service to cause communication of the data from the selected service to the client, where the connection is the client_hello and server_hello (pages 451-454)

Claim 14 is substantially similar to claim 1 and is rejected for the same reasons, where the endpoint is the server, and the ordered list is the CipherSuite.

Claim 15 is substantially similar to claim 3 and is rejected for the same reasons.

In reference to claim 16:

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" discloses the step of establishing a secure connection further comprises the step of establishing the secure connection with the client and endpoint using a cipher suite match, where the establishing of the step is inherent to the client_hello, the "Phase 1, Establish Security Capabilities" and a cipher suite match between the Client Cipher Suite and the Server election. (pages 451-453)

Claim 17 is substantially similar to claim 5 and is rejected for the same reasons.

Claim 19 is substantially similar to claim 7 and is rejected for the same reasons.

Claim 20 is substantially similar to claim 8 and is rejected for the same reasons.

Claim 21 is substantially similar to claim 1 and is rejected for the same reasons, where the endpoint is the server, and the ordered list of encryption types is the CipherSuite.

Claims 23, 24 are substantially similar to claim 1 and are rejected for the same reasons.

Claim 22, 25, and 26 are substantially similar to claim 1 and are rejected for the same reasons.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 4, 9, 11, 18, 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security".

8. Claims 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" and USPGPUB, 2003/0046532, Gast, "System and Method of Accelerating Cryptographically Secure Sessions"

In reference to claim 9:

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" discloses a method as recited in claim 1, wherein the step of selecting an online service further comprises the steps of:

- Determining an encryption type match by finding a first common encryption type in the list of encryption types and the mapping of encryption types to services; (pages 451-453)
- Transmitting the encryption type match to the client; (pages 451-453)

- Selecting a service associated with the encryption type match, where the selection of service is the server's selection of the encryption type. (pages 451-453)

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" fails to disclose:

- Selecting a server farm based on the service; and
- Selecting a particular server in the server farm to provide data to the client.

The Examiner takes official notice that server farms were well known in the art at the time of invention. For Example, access to large corporate sites, or sites that handle heavy traffic cannot deal with the network and computational load with only a single server. Rather, a large set of servers, all operated by that one entity work together to handle the client load. For Example, google.com does not use a single server to handle all the traffic it encounters from use of its search engine. Rather this work is split among a set of servers associated and commonly owned. Each server within the server farm handles the load through a particular distribution method. Ultimately it is a single server that provides data to a client, although which particular server within the farm may change.

It would have been obvious to one of ordinary skill in the art at the time of invention to select a server farm to deal with the large computational loads required by SSL and especially a large number of clients requiring SSL, while selecting a particular server within the server farm to

provide data to the client in order to handle the computational and network burden that a server would not be able to single-handedly provide.

In reference to claim 4:

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" discloses a method as recited in claim 1, further comprising the step of establishing a secure connection with the client, and wherein the receiving step is carried out as part of the establishing step, wherein the step of establishing the secure connection further comprises the step of establishing the secure connection with the client using a cipher suite match, where the establishing of the step is inherent to the client_hello, the "Phase 1, Establish Security Capabilities" and a cipher suite match between the Client Cipher Suite and the Server election. (pages 451-453)

Claim 12 is rejected for the same reasons as claim 13.

In reference to claim 13:

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" discloses a method of providing data associated with a service to a client over a telecommunication network based on SSL encryption capabilities of the client, the method comprising the computer-implemented steps of:

- Receiving from the client as part of an SSL handshake phase message, a request for data and a list of cipher suites that are available at the client. (pages 451-453)

- Matching the cipher suite list received from the client to the mapping to result in identifying at least one cipher suite in common between the cipher suite list and the mapping, where the cipher suite list contains a list of encryption algorithms supported by the client and a match is found by having the server select an algorithm from the list which both parties then decide to use. (pages 451-453)
- Identifying, from the mapping an online service corresponding to the cipher suite in common, where the online service is the actual encryption algorithm that corresponds to the mapping of the list of algorithms (pages 451-453)
- Causing communication of the data from the selected online service to the client over an SSL connection using encryption parameters as defined in the cipher suite in common, where the communication of the data will now employ the algorithm that has been selected along with its relevant parameters. (pages 451-453)

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" fails to disclose:

- Creating and storing, at an SSL termination device, a mapping that associates cipher suites that are supported by the SSL termination device with services that are accessible through the SSL termination device.

USPGPUB, 2003/0046532, Gast, "System and Method of Accelerating Cryptographically Secure Sessions" discloses:

Creating and storing, at an SSL termination device, a mapping that associates cipher suites that are supported by the SSL termination device with services that are accessible through the SSL termination device. (Figure 3, Item 214) & (paragraphs 23 & 34) where the mapping of associated cipher suites is the list of cipher suites supported by the SSL termination device, each of those services accessible through the device.

Gast, paragraph 23 discloses that SSL termination devices provide the ability to have intrusion detection systems monitor the encrypted data stream. Furthermore, it is known that using an SSL termination device would allow for higher loads, since there would be hardware dedicated to SSL processing.

It would have been obvious to one of ordinary skill in the art at the time of invention to use the SSL termination device of Gast which includes the mapping of associated cipher suites in order to allow monitoring of the encrypted data stream or to reduce the computational burden through the use of dedicated hardware.

In reference to claim 18:

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" fails to disclose a method as recited in claim 15, wherein the endpoint is a SSL termination device.

The Examiner takes official notice that SSL termination devices were well known at the time of invention, already developed by several manufacturers, in some cases as dedicated boxes and or processors for SSL.

Furthermore, the Applicant echoes this by disclosing in the specification that SSL termination devices were known in the art at the time of invention and developed by several companies. The Applicant also echoes the well known fact that SSL is a computationally expensive method.

It would have been obvious to one of ordinary skill in the art at the time of invention to use an SSL termination device in order to better handle the computational loads of clients that use SSL connects.

In reference to claim 27:

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" discloses a method of providing data from a service to a client based on encryption capabilities of the client, the method comprising the computer-implemented steps of:

- Receiving an ordered list of cipher suites that corresponds to cipher suites available to a client, wherein a cipher suite match is determined by matching the order list of cipher suites available to a client from the list of cipher suites matched to a list of one or more available services. (pages 451-453)
- Establishing a new SSL connection (pages 451-453)

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" fails to disclose:

- Establishing an SSL connection with an SSL termination module;
- Transmitting to the SSL termination module a request for data and the ordered list of cipher suites;
- Receiving from the SSL termination module a cipher suite match.

The combination of claim 27 is rejected for the same reasons as previously set forth in claim 18. The actions of establishing, transmitting, and receiving, appear to be the identical actions that a regular server would provide in an SSL connection and session, the server's actions being replaced with an SSL termination device instead.

In reference to claim 11:

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" discloses a method of providing data from a service to a client based on encryption capabilities of the client, the method comprising the computer-implemented steps of:

- Receiving an ordered mapping of cipher suite names to services; (pages 451-453)
- Receiving from the client a request for data and an ordered list of cipher suites;
- Determining a cipher suite match by selecting a first common cipher suite in the ordered list of cipher suites and the ordered mappings of cipher suite names to services; (pages 451-453)
- Transmitting the cipher suite match to the client; (pages 451-453)

- Selecting the service associated with the client suite match; (pages 451-453)

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" fails to disclose:

- Selecting a server farm based on the service;
- Selecting a particular server in the server farm to provide the data to the client and transmitting the data to the client.

The following combination in claim 28 however is rejected for the same motivations and reasons as set forth previously in claim 9.

In reference to claim 11:

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" discloses a method of providing data from a service to a client based on encryption capabilities of the client, the method comprising the computer-implemented steps of:

- Receiving an ordered mapping of cipher suite names to services; (pages 451-453)
- Receiving from the client a request for data and an ordered list of cipher suites;
- Determining a cipher suite match by selecting a first common cipher suite in the ordered list of cipher suites and the ordered mappings of cipher suite names to services; (pages 451-453)
- Transmitting the cipher suite match to the client; (pages 451-453)
- Selecting the service associated with the client suite match; (pages 451-453)

"Cryptography and Network Security, Principles and Practice", Stallings, Chapter 14, "Web Security" fails to disclose:

- Selecting a server farm based on the service;
- Selecting a particular server in the server farm to provide the data to the client and transmitting the data to the client.

The following combination in claim 11 however is rejected for the same motivations and reasons as set forth previously in claim 9.

Conclusion

9. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

- A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of the final action and the advisory action is not mailed under after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension pursuant to 37 CFR 1.136(A) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on **(571)272-3799**

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 703-872-9306
Customer Service Representative	Telephone: 571-272-2100	Fax: 703-872-9306

TMH

August 6th, 2006

KAMBIZ ZAND
PRIMARY EXAMINER